Phish or No Phish?

Masquerades, Deception, and Thievery
On the web…

"phishing"

- "***Phishing*** *is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication."*

- *"Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies."*

The term "phishing" is a variant of fishing, probably influenced by p[illegible]

http://en.wikipedia.org/wiki/Phishing (10/16/2012)

Techniques

- Phishing
- Spear Phishing
- Clone Phishing
- Whaling
- Link manipulation
- Filter evasion
- Website forgery
- Phone phishing
- Clone Phishing
- Tab nabbing
- Evil twins
- Click-through syndrome

Phishing success

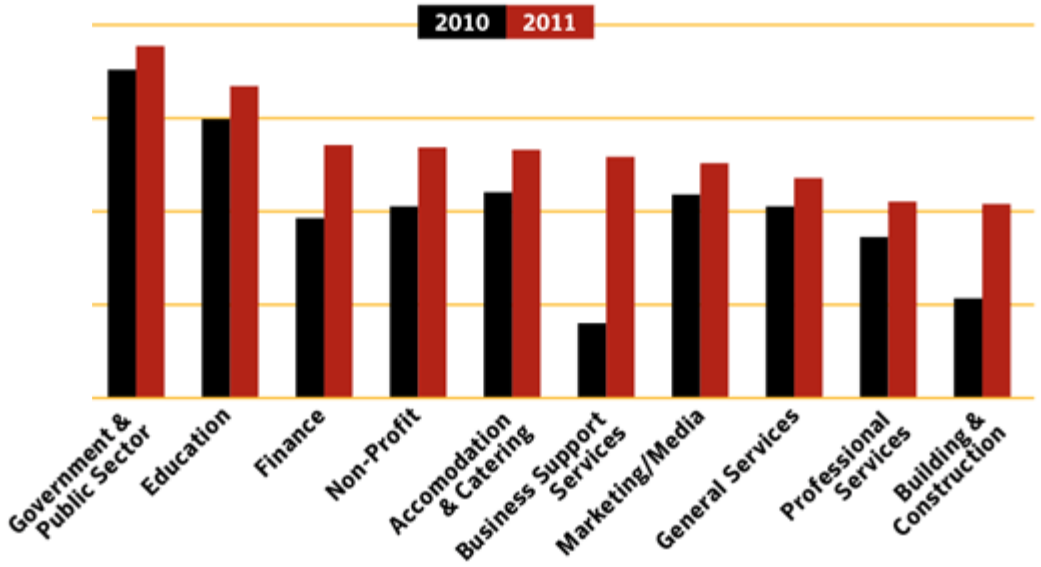
Phishing is profitable with only a low level of success.

- 1% of 1% of a web site's visitors being "phished" can be highly profitable!
- 8:51 PM, 10/16/2012, the "dashboard" for CA.GOV websites indicated 29,752 visitors.
- Deceive 3 people an hour, and a phisher can score one or more of the following profitable items:
  - Personal identity information

Targets

Figure C.24

Proportion Of Email Traffic Identified As Phishing By Industry Sector, 2011

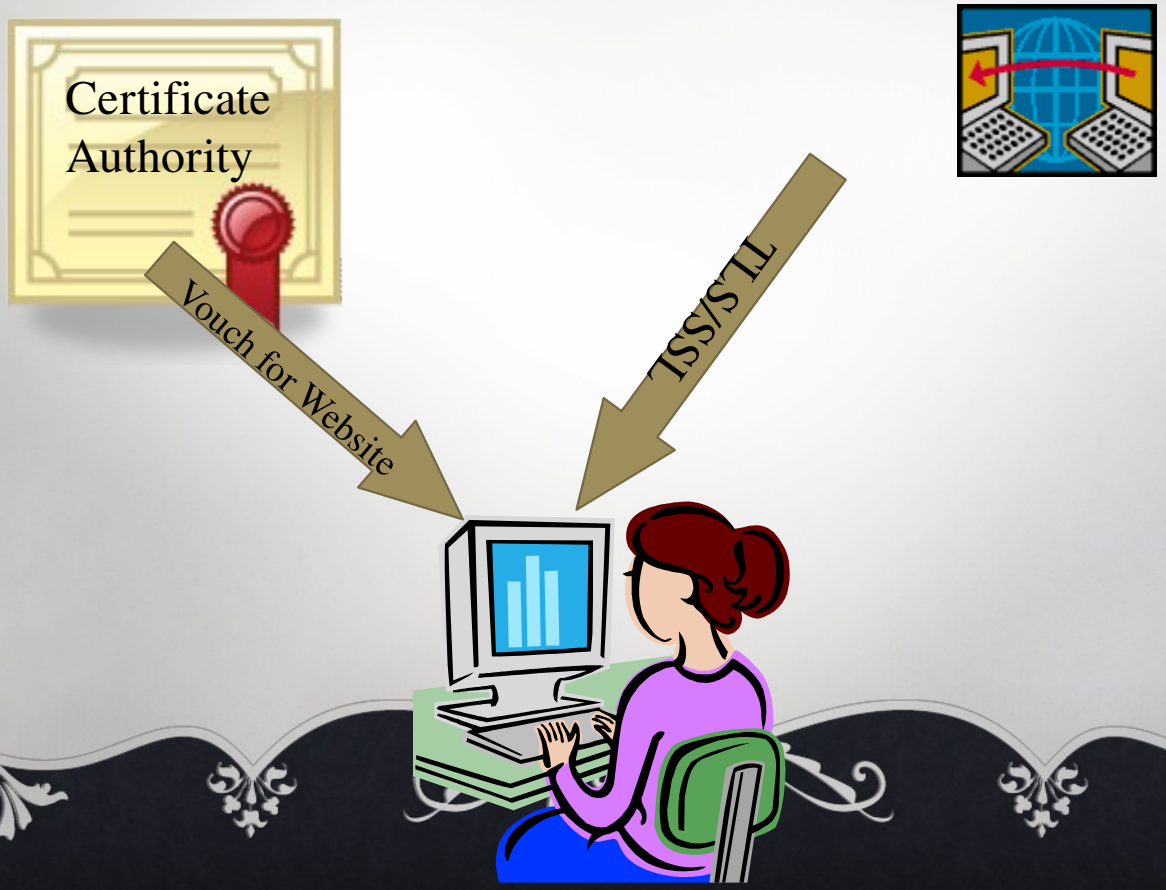


Source: Symantec

Statistics


www.rsa.com/solutions/consumer_authentication/intelreport/11822_Online_Fraud_report_0912.pdf
Phishing Attacks per Month
In August, 49,488 unique phishing attacks were identified by RSA, marking a 17% decrease from July. The bulk of this decrease is a result of fewer phishing campaigns launched against European financial institutions which have accounted for significant spikes in recent months.
60000
50000
40000
30000
20000
10000
0
26907
38970
24019
28365
21119
29974
21030
19141
35558
37878
51906
59406
49488
Aug 11
Sept 11
Oct 11
Nov 11
Dec 11
Jan 12
Feb 12
Mar 12
Apr 12
May 12
Jun 12
Jul 12
Aug 12
Source: RSA Anti-Fraud Command Center

Defense Trifecta



Phish or no phish?

- *The fastest growing Internet game sweeping the nat*

Phish?


Analysis of Phishing Activi
Theft Synonyms, Theft Ant
Phishing - Wikipedia, the f
California Department of M
TheNewBoston - Fre...
What's New in Silver...
Example of custom ...
File Download Progr...
Other bookmarks
Contact Us | Español | Forms | Publications | DMV Info
Search
This Site
California
HOME
OFFICES
ONLINE SERVICES
DRIVER LICENSE
VEHICLE REGISTRATION
Making Your Life EASIER!
Android & iPhone Apps
Important California DMV Alerts
RSS
Tell Us... How Are We Doing?
New Palm Desert Field Office Open
Targeted PSAs Promote Advance Appointments and Online Services
Self Service Terminals Hit 1 Million Transactions
The Latest DMV Office and Closure Information
Online Services
Media Center
Other Services
Make an Appointment before going to a DMV Field Office
Obtain a Copy Online of your Driver Record
Renew Your Vehicle Registration online today
Driver License Renewal
Have you moved? You can submit a Change of Address to DMV online.
Show Detailed Listing of Online Services
How do I...
Select an Item from the List...
Identity Management Portal
LOGIN/REGISTER
Login Here
Register Here
Areas of Interest
Check Us Out!
D M V
PLAY

PHISH?


Driving Lessons...
Watch on DMV You Tube Channel
Important California DMV Alerts
Tell Us... How Are We Doing?
New Palm Desert Field Office Open
Targeted PSAs Promote Advance Appointments and Online Services
Self Service Terminals Hit 1 Million Transactions
The Latest DMV Office and Closure Information
Online Services | Media Center | Other Services
Make an Appointment before going to a DMV Field Office
Obtain a Copy Online of your Driver Record
Renew Your Vehicle Registration online today
Driver License Renewal
Have you moved? You can submit a Change of Address to DMV online.
Show Detailed Listing of Online Services
How do I...
Select an Item from the List...
Identity Management Portal
LOGIN/REGISTER
Login Here
Register Here
Areas of Interest
Check Us Out!
D M V
PLAY

This IS THE Phish!

Get a lock!

What is the “threshold” used for

a website to get an SSL certificate

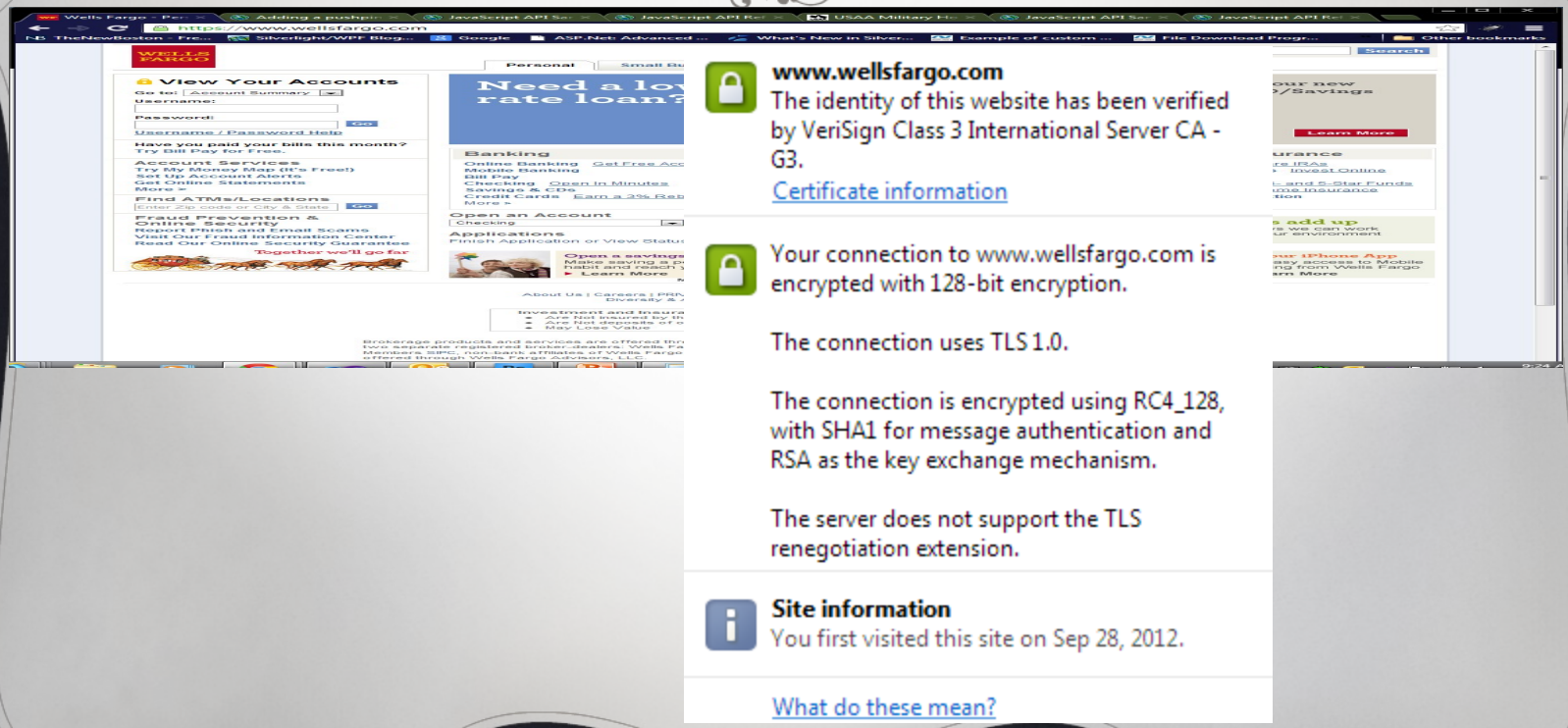
and a “LOCK?”

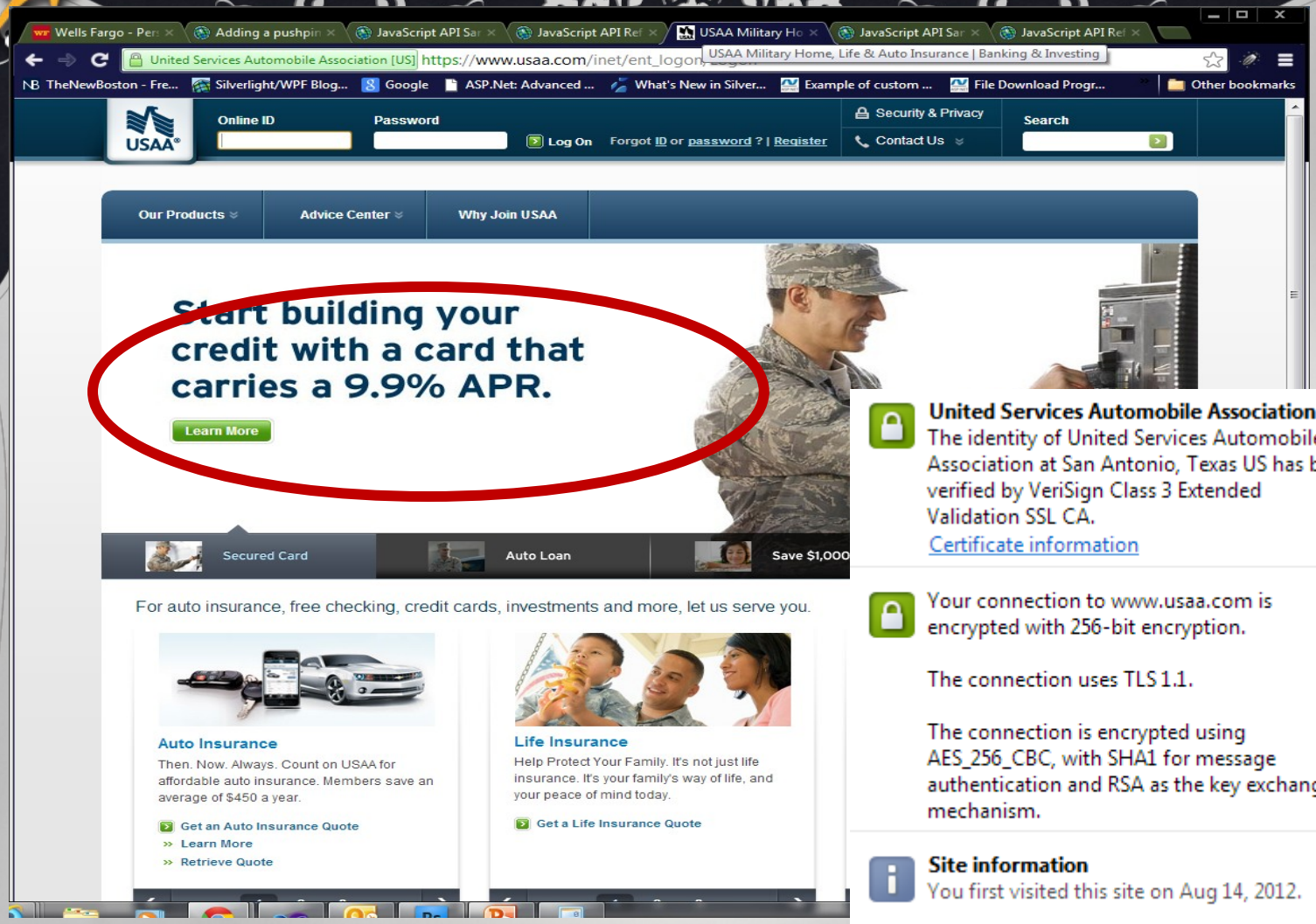
The Ability to Pay.

EV Certificate

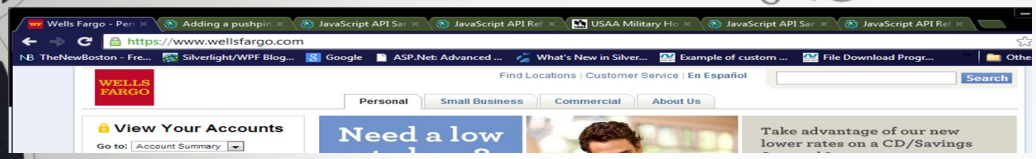
- Focuses on website owner:
  - Official paper trail that backs up your claim that you (1) Own that website, and (2) Own that IP/DNS name, and (3) you are a legal entity.
- User:
  - Offers visual cues for the users that the website employs an EV certificate.

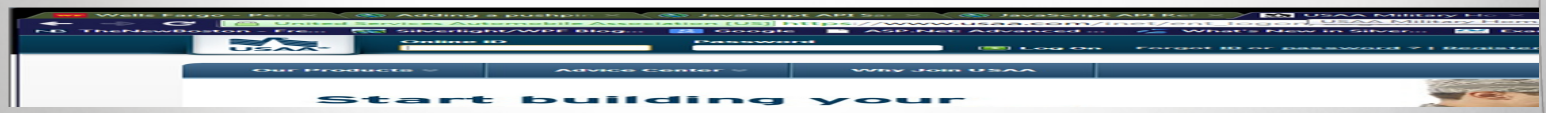
Wells fargo


www.wellsfargo.com
The identity of this website has been verified by VeriSign Class 3 International Server CA - G3.
Certificate information
Your connection to www.wellsfargo.com is encrypted with 128-bit encryption.
The connection uses TLS 1.0.
The connection is encrypted using RC4_128, with SHA1 for message authentication and RSA as the key exchange mechanism.
The server does not support the TLS renegotiation extension.
Site information
You first visited this site on Sep 28, 2012.
What do these mean?


Wells Fargo - Per
Adding a pushpin
JavaScript API Sar
JavaScript API Ref
USAA Military Ho
JavaScript API Sar
JavaScript API Ref
United Services Automobile Association [US] https://www.usaa.com/inet/ent_logon/Logon
USAA Military Home, Life & Auto Insurance | Banking & Investing
TheNewBoston - Fre...
Silverlight/WPF Blog...
Google
ASP.Net: Advanced ...
What's New in Silver...
Example of custom ...
File Download Progr...
Other bookmarks
USAA
Online ID
Password
Log On
Forgot ID or password ? | Register
Security & Privacy
Contact Us
Search
Our Products
Advice Center
Why Join USAA
Start building your credit with a card that carries a 9.9% APR.
Learn More
Secured Card
Auto Loan
Save $1,000
For auto insurance, free checking, credit cards, investments and more, let us serve you.
Auto Insurance
Then. Now. Always. Count on USAA for affordable auto insurance. Members save an average of $450 a year.
Get an Auto Insurance Quote
Learn More
Retrieve Quote
Life Insurance
Help Protect Your Family. It's not just life insurance. It's your family's way of life, and your peace of mind today.
Get a Life Insurance Quote
United Services Automobile Association (wv
The identity of United Services Automobile Association at San Antonio, Texas US has been verified by VeriSign Class 3 Extended Validation SSL CA.
Certificate information
Your connection to www.usaa.com is encrypted with 256-bit encryption.
The connection uses TLS 1.1.
The connection is encrypted using AES_256_CBC, with SHA1 for message authentication and RSA as the key exchange mechanism.
Site information
You first visited this site on Aug 14, 2012.
What do these mean?

Comparison


https://www.wellsfargo.com
WELLS FARGO
Personal
Small Business
Commercial
About Us
View Your Accounts
Need a low
Take advantage of our new lower rates on a CD/Savings


USAA
Start building your


Watch on DMV You Tube Channel

EV SSL Certs…

Web browser
Has built in
Knowledge of
EV CAs

Built-in knowledge
(X.509 standard)

Auditing Entity

Third Party CA

Web Site Certificate

How to implement EV SSL

- Get the certificate from a reputable source.
- Educate your users!!
  - ***Get them to check the address bar.***
- Code your website cleanly!

Phish Tank

http://www.phishtank.com/phish_archive.php

Questions?

- The end